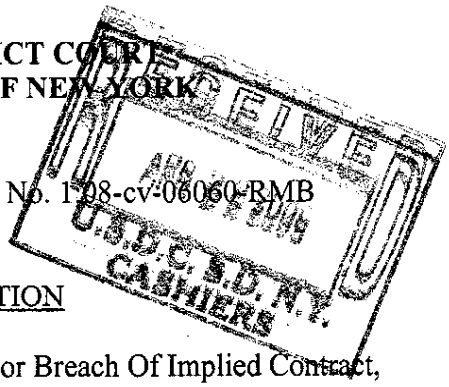
IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK



TOM HAMMOND, WILLIAM H. WICKS, LINDA YOUNG, LOIS GIORDANO, DEBBIE BERNSTEIN, ALYSON KANNEY, and KEN WITEK, on behalf of themselves and all others similarly situated, Plaintiffs vs. THE BANK OF NEW YORK MELLON CORPORATION, Defendant	Civil Action No. 1:08-cv-06060-RMB CLASS ACTION Complaint For Breach Of Implied Contract, Negligence, Negligence *Per Se*, and Violations of the California, Illinois, Michigan, New Jersey and New York Consumer Protection Acts JURY TRIAL DEMANDED

PLAINTIFFS' SECOND AMENDED CLASS ACTION
COMPLAINT AND JURY DEMAND

Plaintiffs Tom Hammond, William H. Wicks, Linda Young, Lois Giordano, Debbie Bernstein, Alyson Kanney, and Ken Witek (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their attorneys, allege as follows:

INTRODUCTION

1. This is a class action lawsuit brought on behalf of Plaintiffs, individually, and on behalf of similarly situated consumers or entities whose names, addresses, Social Security numbers, bank account information, financial data, debit or credit card, checking account numbers and information and/or shareholder account information (the "Sensitive Personal Information") was stolen, accessed and/or compromised by third parties while entrusted to Defendant The Bank of New York Mellon Corporation ("BNY"). BNY processes payments on behalf of its corporate customers, and provides stock transfer, employee plan administration and

related services for issuers of securities, such as the Walt Disney Company. BNY also processes payments on behalf of customers of utility companies, such as the Borough of Avalon and American Water Co. and other establishments like the Vesper Club. In connection with these duties, BNY comes into the possession of – and is entrusted with – the Sensitive Personal Information of millions of consumers from across the United States.

2. In or around February 2008, a BNY metal box with six to ten unencrypted computer back-up tapes containing the Sensitive Personal Information of consumers was "lost" from a truck operated by a transport company hired by BNY. BNY initially reported that these "lost" back-up tapes contain the Sensitive Personal Information of Plaintiffs and approximately 4.5 million other consumers. Upon information and belief, BNY did not begin notifying the affected consumers of the February 2008 data breach until several weeks later, and is still in the process of notifying all of the consumers whose Sensitive Personal Information was compromised.

3. When it initially began notifying the affected consumers about the loss of their Sensitive Personal Information, BNY offered them the opportunity to receive free credit monitoring for a period of 12 months. On or around May 21, 2008, Richard Blumenthal, the Attorney General for the State of Connecticut, sent a letter to BNY's general counsel addressing the data breach and BNY's proposed remedy. A copy of this letter is attached as Exhibit A. Attorney General Blumenthal described BNY's proposed one year worth of credit monitoring as "grossly inadequate."

4. Yet another security breach occurred on or around April 29, 2008, again involving the Sensitive Personal Information of consumers entrusted to BNY. This time, a backup data storage tape containing images of scanned checks and other payment documents was "lost"

while being transported from Philadelphia to Pittsburgh. It is unknown how many individual customers were affected by the second breach, but it has been reported that it involved data from forty-seven (47) BNY institutional clients. In a letter to consumers, BNY revealed that this second breach "may include Sensitive Personal Information about you, such as name, address and social security number." A copy of this letter, which was received by Plaintiff Linda Young on or around June 9, 2008, is attached as Exhibit B.

5. BNY's initial statements that the back-up tapes that were lost in the February 2008 data breach contained the Sensitive Personal Information of approximately 4.5 million consumers were materially false and misleading. On or around August 28, 2008 – subsequent to the filing of this complaint, and nearly *7 months* after the information was initially "lost" – BNY revealed that the Sensitive Personal Information of an additional 8 million consumers and businesses could have been compromised as a result of the February data breach. In a press release related to these additional details about this "shocking security breach," the Connecticut Attorney General's Office indicated that it was "appalled" and "outraged" by BNY's months-long delay in informing consumers that their Sensitive Personal Information had been lost.

6. Upon information and belief, BNY still has not completely and accurately disclosed the full extent of the data breaches, nor has it accurately characterized the real risk of identity theft to which Plaintiff and the Class members are subjected. BNY insists that these unencrypted tapes were simply "lost," and that there is no evidence of misuse of the information. Indeed, the BNY website devoted to the breaches prominently states "**[a]t the time of the incidents, we said there were no indications that the data had been accessed or misused in any way — and that remains the case."**

7. However, after the data breaches, Plaintiff Hammond has had two different unauthorized charges appear on his credit card. When Plaintiff Hammond called BNY's toll-free data breach hotline, he was informed that the tapes indeed contain Visa and MasterCard numbers, and provided Hammond with a BNY mailing address in Georgia where he could send his credit card statements reflecting the unauthorized charges. Upon information and belief, BNY has never publicly disclosed that credit or debit card information was involved in the data breaches.

8. Plaintiffs bring this lawsuit for the purpose of securing full, appropriate and meaningful relief based on BNY's negligent, fraudulent, reckless, wrongful, and unlawful conduct including, *inter alia*:

a. Relief for the actual injuries suffered by Plaintiffs and the Class members as a result of BNY's failure to provide adequate safeguards to protect their Sensitive Personal Information, which would have prevented such widespread data breaches from occurring in the first place. Plaintiffs also seek prospective equitable relief to ensure that BNY takes the necessary measures to make certain that such massive data breaches do not reoccur in the future.

b. Relief for BNY's inexplicable delays in announcing and notifying Plaintiffs and the Class members of the February 2008 and April 2008 data breaches. BNY's unreasonable delays prevented and/or hindered Plaintiffs and the Class members from taking immediate steps to monitor and safeguard their Sensitive Personal

Information. Upon information and belief, BNY *still* has not notified all of the affected consumers that their Sensitive Personal Information was compromised in the February 2008 data breach.

c. Meaningful and appropriate relief on a going forward basis on behalf of Plaintiffs and the Class members. BNY's offer to provide affected consumers with free credit monitoring for only two years, $25,000 of identity fraud insurance to all non-New York residents, and reimbursement for a single credit freeze and one removal are wholly inadequate and insufficient. Plaintiffs further seek to ensure that *all* of the affected consumers receive prompt, complete and accurate disclosures regarding the precise Sensitive Personal Information that was lost and/or compromised.

9. As a result of BNY's wrongful conduct, millions of consumers across the United States have had their Sensitive Personal Information compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identity theft and otherwise suffered damages including, without limitation, the (i) cost of obtaining identity theft insurance, (ii) cost of comprehensive credit monitoring (over and above the credit monitoring offered by BNY), (iii) the cost of obtaining credit reports,[1] (iv) monetary losses resulting from the unauthorized use of their Sensitive Personal Information, (v) time and out-of-pocket expenses incurred to repair their damaged credit (including multiple credit freezes), (vi) loss of the value of their Sensitive Personal Information, (vii) loss of control of their Sensitive Personal Information, (viii) fear and

[1] Consumers are entitled to a single free credit report once every 12 months.

apprehension of fraud, loss of money and identity theft, and (ix) other economic and non-economic damages.

10. BNY's wrongful actions and/or inaction constitute violations of the consumer protection statutes of California, Illinois, Michigan, New Jersey and New York, and also constitute breach of implied contract, breach of fiduciary duty, negligence *per se* and negligence under California, Illinois, Michigan, New Jersey, New York and Pennsylvania common law and the common law of all other States.

11. This case is brought to ensure that the consumers affected by the massive BNY data breaches are appropriately compensated and adequately protected from the real risk of future misuse of their Sensitive Personal Information. These are not trivial or inconsequential concerns. Indeed, Connecticut Attorney General Blumenthal's May 21, 2008 letter to BNY describes the February 2008 breach as "highly dangerous, indeed possibly devastating," and expresses concerns with "the possibility that credit card fraud and identity loss may result from the breach of this sensitive and personally identifying information."

PARTIES

12. Plaintiff Alyson Kanney ("Kanney") is a resident of New York City. By letter dated June 9, 2008, Kanney received notice from BNY that her personal and sensitive information, including her Social Security number, was compromised in one of the data breaches that occurred in or around February of 2008.

13. In November 2008, an unauthorized credit card account was opened in Kanney's name, using her Social Security number, with Capital One.

14. On November 19, 2008, Kanney filed a police report with the New York City Police Department regarding the unauthorized use of her personal information, including her Social Security number, to open a credit card account with Capital One.

15. By letter dated November 26, 2008, Kanney contacted BNY and informed them that an unauthorized credit card account was opened in her name using her Social Security number, and that she was a victim of identity theft.

16. Kanney was subsequently contacted by a Bill Valentine who stated he was an investigator acting on behalf of BNY. Mr. Valentine asked Kanney questions about the unauthorized Capital One account. They discussed the missing BNY data tapes, and Mr. Valentine stated that "they hoped to catch the person that did this." Kanney provided Mr. Valentine with the telephone number of the New York City detective investigating her complaint. She never heard from Mr. Valentine – or any other BNY investigator – again regarding this matter.

17. Kanney has never experienced identity theft and/or unauthorized credit transactions at any time prior to the BNY security breach in February 2008.

18. Plaintiff Tom Hammond ("Hammond") is a resident of Auburn Hills, Michigan. In or around May 2008, Hammond received a letter from BNY informing him that his Sensitive Personal Information was contained on one of the back-up data tapes that was involved in the February 2008 data breach. A true and correct copy of the letter received by Hammond (with his personal activation code redacted) is attached hereto as Exhibit C. As a direct and/or proximate result of BNY's wrongful conduct alleged herein, Hammond suffered injuries including, *inter alia*, Hammond's private, nonpublic personal and financial information was improperly and illegally compromised and/or disseminated to third parties; BNY wrongfully prevented

Hammond from taking prompt measures to protect himself through BNY's unreasonable delay in notifying Hammond about the data breaches; and the remedies offered by BNY are insufficient to make Hammond whole or otherwise adequately protect him from identity theft and/or future damages, all of which have caused him to suffer from distress and disturbance to his peace of mind.

19. Subsequent to the February 2008 data breach, Hammond experienced two unauthorized charges on his credit card. In July 2008, a charge of approximately $12 appeared on his credit card statement from an internet company that he has never heard of, and to which he never provided his Sensitive Personal Information. He was also assessed another similar unauthorized charge in August 2008.

20. Upon reviewing his credit card statement and finding the unauthorized charges, Hammond called the toll-free number provided by BNY. When he asked the BNY representative to tell him what information was compromised as part of the data breaches, he was told that Visa and Master Card credit card numbers are included. Upon information and belief, BNY has never publicly revealed that credit or debit card numbers were included in the information that was compromised. Instead, the BNY letter Hammond received simply stated that the "missing tapes contained certain personal information, such as your name, address, Social Security number and/or shareholder account information…" *See* Exhibit C. Hammond was never informed that he should monitor and/or cancel any of his credit card accounts.

21. To date, Hammond has spent a substantial amount of time attempting to remedy the unauthorized charges levied on his credit card account. He also incurred charges on his cell phone for making calls necessary to address the unauthorized charges.

22. Plaintiff Linda Young ("Young") is a resident of Ellwood City, Pennsylvania. On or around June 9, 2008, Young received a letter from BNY notifying her that an unencrypted back-up tape that "may" include Young's Sensitive Personal Information was "lost" while being transported from BNY's processing site in Philadelphia to its data storage site in Pittsburgh. As a direct and/or proximate result of BNY's wrongful conduct alleged herein, Young suffered injuries including, *inter alia,* Young's private, nonpublic personal and financial information was improperly and illegally compromised and/or disseminated to third parties; BNY wrongfully prevented Young from taking prompt measures to protect herself through BNY's unreasonable delay in notifying Young about the data breaches; and the remedies offered by BNY are insufficient to make Young whole or otherwise adequately protect her from identity theft and/or future damages, all of which have caused her to suffer from distress and disturbance to her peace of mind.

23. Plaintiff William H. Wicks ("Wicks") is a resident of Manilus, New York. Wicks was notified by BNY Mellon Shareowner Services that his Sensitive Personal Information was contained on one of the missing tapes. As a direct and/or proximate result of BNY's wrongful conduct alleged herein, Wicks suffered injuries , including, *inter alia,*, Wicks' private, nonpublic personal and financial information was improperly and illegally compromised and/or disseminated to third parties; BNY wrongfully prevented Wicks from taking prompt measures to protect himself through BNY's unreasonable delay in notifying Wicks of the data breaches; and the remedies offered by BNY are insufficient to make Wicks whole or otherwise adequately protect him from identity theft and/or future damages, all of which have caused him to suffer from distress and disturbance to his peace of mind.

24. Plaintiff Lois Giordano ("Giordano") is a resident of Hammonton, New Jersey. Giordano was notified by BNY Mellon Shareowner Services that her Sensitive Personal Information was contained on one of the missing tapes. As a direct and/or proximate result of BNY's wrongful conduct alleged herein, Giordano suffered injuries including, *inter alia*, Giordano's private, nonpublic personal and financial information was improperly and illegally compromised and/or disseminated to third parties; BNY wrongfully prevented Giordano from taking prompt measures to protect herself through BNY's unreasonable delay in notifying Giordano about the data breaches; and the remedies offered by BNY are insufficient to make Giordano whole or otherwise adequately protect her from identity theft and/or future damages, all of which have caused her to suffer from distress and disturbance to her peace of mind.

25. Plaintiff Debbie Bernstein ("Bernstein") is a resident of Santa Monica, California. Bernstein was notified by BNY Mellon Shareowner Services that her Sensitive Personal Information was contained on one of the missing tapes. As a direct and/or proximate result of BNY's wrongful conduct alleged herein, Bernstein suffered injuries including, *inter alia*, Bernstein's private, nonpublic personal and financial information was improperly and illegally compromised and/or disseminated to third parties; BNY wrongfully prevented Bernstein from taking prompt measures to protect herself through BNY's unreasonable delay in notifying Bernstein about the data breaches; and the remedies offered by BNY are insufficient to make Bernstein whole or otherwise adequately protect her from identity theft and/or future damages, all of which have caused her to suffer from distress and disturbance to her peace of mind. Bernstein is the custodian of her daughter's Disney shareholder account, and her Sensitive Personal Information may have been compromised as a result of the breach as well.

26. Plaintiff Ken Witek is a resident of Algonquin, IL. Witek was notified by BNY Mellon Shareowner Services that his Sensitive Personal Information was contained on one of the missing tapes. As a direct and/or proximate result of BNY's wrongful conduct alleged herein, Witek suffered injuries , including, *inter alia,*, Witek's private, nonpublic personal and financial information was improperly and illegally compromised and/or disseminated to third parties; BNY wrongfully prevented Witek from taking prompt measures to protect himself through BNY's unreasonable delay in notifying Witek of the data breaches; and the remedies offered by BNY are insufficient to make Witek whole or otherwise adequately protect him from identity theft and/or future damages, all of which have caused him to suffer from distress and disturbance to his peace of mind.

27. Defendant BNY is a Delaware corporation with its principal place of business located at One Wall Street, New York, New York 10286. BNY describes itself as "a global financial services company focused on helping clients manage and service their financial assets, operating in 34 countries and serving more than 100 markets." BNY further boasts that "[t]he company is a leading provider of financial services for institutions, corporations and high-net-worth individuals, providing superior asset management and wealth management, asset servicing, issuer services, clearing services and treasury services through a worldwide client-focused team." According to its most recent Form 10-K filed with the Securities and Exchange Commission, BNY was created on July 1, 2007 following a merger of The Bank of New York Company, Inc. and Mellon Financial Corporation. BNY has approximately $1.121 trillion of assets under management, and $23.1 trillion in assets under custody and administration. BNY common stock is publicly traded on the New York Stock Exchange under the ticker "BK." BNY and its subsidiaries have over 42,000 employees.

JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and this action is a class action in which some members of the Class are citizens of states different from the states of which BNY is a citizen. *See* 28 U.S.C. § 1332(d)(2)(A).

29. This Court has personal jurisdiction over BNY because it owns and operates a business located within the State of New York, and conducts substantial business throughout the United States and the State of New York, including the Southern District of New York.

30. Venue properly lies in the Southern District of New York, pursuant to 28 U.S.C. § 1391(a)(2), because a substantial part of the acts giving rise to Plaintiffs' claims occurred in the Southern District of New York and because BNY is headquartered and conducts substantial business in the geographic area encompassed by this judicial district.

FACTUAL BACKGROUND

31. In connection with the functions it performs on behalf of its institutional and corporate clients, BNY is entrusted with the confidential Sensitive Personal Information of millions of people. Many of BNY's clients contract with BNY to administer services concerning shareholders. By way of example, it has been reported that People's United Bank ("People's United") provided BNY with the Sensitive Personal Information of its shareholders/depositors as part of the process of converting People's United into a public company. People's United was reportedly required to provide all of its shareholders/depositors with the opportunity to vote on the conversion; BNY was provided with their Sensitive Personal Information so that it could disseminate and tabulate their votes.

32. BNY has expressly and/or impliedly represented that it would take appropriate measures to safeguard the Sensitive Personal Information of Plaintiffs and the Class members. For example, the current Privacy Policy on BNY's website claims that the "we take the issue of privacy very seriously." Likewise, BNY's Online Privacy Policy states that "[w]e want to assure that visitors to our Web site have the security, privacy and confidentiality that they expect from a premier financial services institution." Additionally, the BNY form letter received by Hammond in May 2008 tells him to "be assured that we take the protection of your information very seriously and have taken additional measures to protect your account with us." BNY's website also refers to its "internal policies governing use and disclosure of such confidential information" to reassure the public about its ability to maintain the security of confidential information. These representations and others by BNY created a duty by BNY to protect the Sensitive Personal Information of Plaintiffs and the Class members.

33. Upon information and belief, Plaintiffs and the Class members are required to provide BNY with their Sensitive Personal Information in order to receive the benefit of BNY's services. For example, shareholders of Walt Disney Company common stock must, upon information and belief, provide BNY with their Social Security numbers for tax and other identification purposes.

A. The February 2008 Data Breach.

34. The first BNY data breach occurred in February 2008. On February 27, 2008, an archive service vendor selected by BNY to transfer the confidential Sensitive Personal Information of Plaintiffs and the Class members informed BNY that it "could not account for one of several boxes of data backup tapes that they were transporting to an off-site storage facility." The six to ten unencrypted data backup tapes that were in the missing box contained,

among other things, the Social Security numbers of millions of consumers. Upon information and belief, this data breach occurred in New Jersey and involved data from BNY's Shareholder Services unit.

35. Inexplicably, BNY unreasonably delayed notifying consumers, the primary owners of the Sensitive Personal Information, of the February 2008 data breach. In his May 21, 2008 letter to BNY, Connecticut Attorney General Blumenthal wrote that "I am especially concerned by the delay in informing consumers, possibly heightening the risks of wrongdoing. Neither [People's United], nor its customers were promptly notified. Even now, many may be in the dark."

36. It has been reported that BNY took more than eight (8) weeks to notify the affected institutions of the February 2008 data breach. Even more astounding is the fact that many consumers who were potentially impacted by this incident *still have not received letters from BNY* notifying them of the breach and cautioning them that their Sensitive Personal Information was compromised. Needless to say, it is critical for these consumers to be promptly notified that their Sensitive Personal Information has been (or may have been) jeopardized so that they can take appropriate steps to protect their identity, such as immediately implementing a credit freeze and/or closely monitoring their credit reports.

37. Upon information and belief, many consumers who have attempted to contact BNY have been unable to get a straight answer as to whether their Sensitive Personal Information was actually compromised by the data intrusion.

38. In the aftermath of the February 2008 data breach, BNY initially offered consumers twelve (12) months worth of free credit monitoring. According to one of the letters

that was sent to consumers by BNY after the breach, consumers were given ninety (90) days from the date of the letter to enroll in the free credit monitoring program offered by BNY.

39. Based on BNY's representations, on May 30, 2008, Attorney General Blumenthal's office – in connection with the Connecticut Department of Consumer Protection – issued a press release identifying the "top 25 companies with the most Connecticut residents affected by the Bank of New York Mellon data breach." These companies are listed below, with the approximate number of affected Connecticut residents in parentheses:

- People's United Financial Inc. **(403,894)**
- John Hancock Financial Services, Inc. *(acquired by Manulife Financial Corporation)* **(33,586)**
- The Walt Disney Company **(18,361)**
- TD Bank Financial Group **(9,389)**
- The Bank of New York Mellon Corporation **(3,324)**
- Hudson United Bancorp *(acquired by TD Bank Financial Group)* **(2,703)**
- United Parcel Service, Inc. **(2,075)**
- Wachovia Corporation **(1,479)**
- MetLife, Inc. **(1,373)**
- Hudson City Bancorp **(601)**
- Eastman Kodak Company **(456)**
- Burlington Resources *(acquired by ConocoPhillips Inc.)* **(447)**
- Providian Financial *(acquired by Washington Mutual, Inc.)* **(404)**
- Penn Fed Financial *(acquired by New York Community Bancorp)* **(360)**
- ADESA, Inc. **(277)**

- Alcatel-Lucent **(243)**
- Odyssey America Reinsurance Corporation **(232)**
- Seacoast Financials Services Corp. *(acquired by Sovereign Bancorp)* **(216)**
- Viewpoint Bank **(213)**
- Diamond Shamrock *(acquired by ConocoPhillips Inc.)* **(211)**
- Sound Federal Bancorp *(acquired by Hudson City Bancorp)* **(199)**
- Big Lots, Inc. **(192)**
- Guidant Corporation *(acquired by Boston Scientific Corp)* **(126)**
- New York Community Bancorp **(126)**
- ACE Ltd. **(119)**

40. In all, BNY initially reported that the February 2008 data breach involved the Sensitive Personal Information of consumers, investors and/or employees of more than seven hundred (700) companies and institutions. According to BNY's reports at the time, the Sensitive Personal Information of some 4.5 million consumers nationwide was compromised by the February 2008 data breach. On information and belief, however, BNY has not provided a breakdown of the number of companies and/or residents of each of the other states affected by the February 2008 data breach as it did for the Connecticut Attorney General.

41. As discussed *infra,* it was not until late August 2008 that BNY revised these figures and reported that the February 2008 data breach was actually much larger, involving the Sensitive Personal Information *of an additional 8 million Class members nationwide*. According to a September 2, 2008 press release by the Connecticut Attorney General's Office, BNY "lost the personal information of 135,000 more Connecticut residents in the February 2008 data

breach than it originally reported…." The press release reported that "[t]he lost information for the latest 135,000 Connecticut residents is mostly Social Security numbers."

42. Based on the current figures revealed by BNY, there are 635,000 residents in Connecticut alone – and 12.5 million nationwide – whose Sensitive Personal Information was "lost" in the February 2008 data breach. Through no fault of their own, all of these individuals are now at a substantially increased risk of identity theft and fraud.

B. The April 2008 Data Breach.

43. Failing to learn its lesson from the February 2008 data breach, and adding insult to injury, the confidential Sensitive Personal Information of consumers entrusted to BNY was subject to yet another data breach on or around April 29, 2008. On this occasion, as reported by BNY, an unencrypted back-up tape that "may" contain consumers' Sensitive Personal Information was "lost while being transported by an outside carrier from [BNY's] processing site in Philadelphia, PA to its data storage site in Pittsburgh, PA."

44. The April 2008 data breach reportedly involved data from forty-seven (47) of BNY's institutional clients and a yet to be determined number of individual consumers. Upon information and belief, the April 2008 incident involved a different business unit of BNY: the BNY Mellon Working Capital Solutions unit. This unit is reportedly responsible for processing payments on behalf of BNY's institutional clients, such as pension funds and mutual funds.

45. Yet again, BNY delayed notifying consumers, the primary owners of the Sensitive Personal Information, of the data breach. It has been reported that BNY did not complete notifying the forty-seven (47) institutional clients affected by the April 2008 data breach until May 16, 2008. Plaintiff Young's Sensitive Personal Information was at risk of being compromised as a result of the April 2008 data breach, yet she did not receive a letter from

BNY informing her that her Sensitive Personal Information may have been compromised until June 7, 2008 – nearly 6 weeks after the data breach occurred and several weeks after BNY finished first notifying its corporate clients.

46. The June 7, 2008 BNY letter to Plaintiff Young states that BNY is implementing certain unspecified "additional security procedures" to help ensure that there is not another data breach. In addition, BNY offered Young and the other recipients of this ostensible form letter an opportunity to receive "credit report monitoring services for two years, at no cost," identity theft insurance (where not prohibited by state law, such as in New York) of up to $25,000 and the cost of "the initial placement and one removal" of a credit freeze.

C. BNY Belatedly Reveals that 8 Million More People Are Affected by the Data Breaches.

47. At no point when BNY initially disclosed the February 2008 data breach did it reveal that the total number of consumers affected by the breach – reported to be approximately 4.5 million by BNY at the time – would actually be nearly three times the initial estimates. Indeed, upon learning of this recent revelation about the substantially increased size of the breach, Connecticut Department of Consumer Protection Commissioner Jerry Farrell, Jr. reportedly remarked that "[n]othing in the data we were given in May and June by BNY Mellon indicated in any way that these additional six million individuals and businesses were involved."

48. On or around August 28, 2008, BNY made the shocking revelation that there were approximately 12.5 million consumers and entities nationwide whose Sensitive Personal Information was compromised as a result of the breaches. According to the Identity Theft Resource Center, an advocacy group based in California, this revised figure made the two BNY data breaches the largest reported data breaches in the United States in 2008 as measured by the number of exposed records.

49. A press release issued by the Connecticut Attorney General's Office reacted to BNY's recent belated disclosure with outrage, remarking that BNY "fumbled yet again, severely mishandling this serious information loss, a potential financial nightmare for consumers." The Connecticut Attorney General's Office reportedly issued subpoenas to third parties Webster Bank and Wachovia in connection with its investigation.

50. In addition to BNY's inaccurate initial statements about the scope of the data breaches, BNY has not fully and accurately revealed what actually happened to the "lost" information, nor disclosed precisely what information was involved in the breaches. In a Question and Answer section on BNY's website devoted to addressing consumers' concerns about the data breaches, BNY explains that the back-up data storage tapes were simply lost while in the possession and control of a third-party transport company:

> **Why are these tapes missing? What happened?**
>
> In both incidents, back-up data storage tapes were discovered missing while being transported by a third-party courier.[2]

51. Likewise, in letters from BNY to Class members concerning both data breaches, BNY points the finger at the transport company as being responsible for losing the Sensitive Personal Information. *See, e.g.,* Exhibit B (the unencrypted back-up tape containing the Sensitive Personal Information "was lost while being transported by an outside carrier from [BNY's] processing site in Philadelphia, PA to its data storage site in Pittsburgh, PA."); Exhibit C ("On February 27, 2008, our archive services vendor notified us that they could not account for one of several boxes of data backup tapes that they were transporting to an off-site storage facility.").

[2] *See* http://www.bnymellon.com/tapequery/faqs.html (last visited on September 18, 2008).

52. BNY's Question and Answer section on its website also says nothing about credit and debit card information being included in the breaches:

> **What kind of data was on the missing tapes?**
>
> The missing back-up tape from Shareowner Services included shareholder and plan participant account information, such as name, mailing address, Social Security number and transaction activity.
>
> The missing back-up tape from Working Capital Solutions consisted of images of scanned checks and other related payment documents involved in the delivery of wholesale lockbox processing services. Most of the checks were in connection with commercial or other business-to-business payments, though some were related to consumer payments as well.
>
> For more background on these incidents, *see* Additional Information.[3]

53. At least one consumer (Plaintiff Hammond) has been the victim of identity theft after the February 2008 data breach, and was informed by a BNY representative on the telephone that credit card information, in fact, is included in the lost information.

54. To date, the "lost" unencrypted data tapes have not been found or accounted for.

D. BNY's Inadequate Remedial Scheme.

55. BNY is currently offering eligible consumers, who affirmatively contact BNY and elect to accept them within ninety (90) days of receiving BNY's letter, the following remedial services:

- Credit monitoring services for 2 years. BNY engaged ConsumerInfo.com to provide Class members with its Triple Alert Credit Monitoring product, which includes daily monitoring of credit reports from the three major consumer reporting companies (Equifax, Experian, and TransUnion). In order to obtain these services, Class members are asked to again provide their Sensitive Personal Information

[3] *Id.*

(including their Social Security numbers) – which BNY already has, and which information many consumers are understandably reluctant to provide once again.

- Identity theft insurance in the amount of $25,000. Significantly, BNY is not offering any identity theft insurance-type compensation to residents of New York or other affected states who cannot receive identity theft insurance because of restrictions under state law.

- A toll free hotline that is purportedly open six (6) days a week that consumers can call with inquiries.

- Cost of the initial placement and one removal of a credit freeze.

56. Under the circumstances, the above remedial scheme offered by BNY is wholly inadequate and insufficient to appropriately compensate and protect Plaintiffs and the Class members from the substantially increased risk of identity theft.

i. Costs Associated with Freezing and Unfreezing Credit Accounts Are Not Adequately Accounted for in the BNY Remedial Scheme.

57. A "credit freeze" is a service provided by credit rating agencies – for a fee – whereby a consumer's credit is "frozen," making it impossible for anyone, including the consumer, to take out a new line of credit or to open up a new credit card account. If the consumer wishes to obtain new credit, or if the consumer is involved in any transaction that requires another party to access their personal credit report, he or she typically pays another fee to temporarily or permanently "unfreeze" their credit information.

58. In order to obtain a credit freeze, consumers must write to all three (3) of the credit reporting bureaus (Experian, Equifax, and TransUnion) to request that a freeze be placed on their credit accounts. The consumer must provide each of the credit reporting agencies with

their full name, Social Security number, date of birth, current address and previous addresses for the past two years, the applicable fee (or incident report from a law enforcement agency), a copy of a government issued identification card and a copy of a utility or other bill with the consumers' current address. While BNY has offered to pay the "cost of the initial placement and one removal" of a credit freeze, it has not indicated whether it will reimburse Class members for the postage fees associated with mailing the credit freeze requests to all three of the credit reporting bureaus or for the time and expense required to copy the government issued identification card and utility bill.

59. Each of the credit reporting agencies charge a fee to place, lift or remove a credit freeze unless the consumer (or consumer's spouse) is a victim of identify theft and submits a valid police report related to the identity theft.

60. Residents of Kentucky, Nebraska, Pennsylvania, and South Dakota, for example, can only place a credit freeze on their personal credit reports for a period of seven (7) years. After the expiration of this time period, consumers in these states who wish to place a credit freeze on their credit accounts must once again contact all three (3) credit reporting agencies, pay each of them the applicable fee to freeze their account, and go through the hassle of providing each of the agencies with proof of their identity (by copying government issued photos and utility bills).

61. Residents of most states are charged a fee by each of the three (3) credit reporting agencies every time they temporarily remove a credit freeze (unless the consumer can provide a valid copy of an identity theft report filed with a law enforcement agency). For example, Experian charges the following fees for temporarily removing a credit freeze:

- $10.00 for each temporary credit freeze removal for residents of Alabama, Alaska, Arkansas, California, Colorado, Florida, Illinois, Kansas, Kentucky, Maine, Michigan, Mississippi, Nevada, New Hampshire, North Carolina, Oklahoma, Oregon, Rhode Island, Utah, Washington, Wisconsin and Wyoming.

- $10.60 (including taxes) for each temporary credit freeze removal for residents of Connecticut, South Carolina and South Dakota.

- $10.70 (including taxes) for each temporary credit freeze removal for residents of Pennsylvania and Puerto Rico.

- $10.83 (including taxes) for each temporary credit freeze removal for residents of Texas.

- $12.00 for each temporary credit freeze removal for residents of Iowa.

- $6.00 for each temporary credit freeze removal for residents of Idaho.

- $5.00 for each temporary credit freeze removal for residents of Arizona, Maryland, Massachusetts, Minnesota, Missouri, New Jersey, North Dakota, Ohio and Vermont.

- $5.20 (including taxes) for each temporary credit freeze removal for residents of Hawaii.

- $5.25 (including taxes) for each temporary credit freeze removal for residents of New Mexico.

- $5.30 (including taxes) for each temporary credit freeze removal for residents of West Virginia.

- $5.41 (including taxes) for each temporary credit freeze removal for residents of New York.

- $8.00 for each temporary credit freeze removal for residents of Louisiana.

- $8.00 for each temporary credit freeze removal for residents of Georgia and Montana.

62. Upon information and belief, the other two credit reporting agencies (Trans Union and Equifax) also charge similar fees for temporarily removing a credit freeze.

63. Residents of most states typically are charged another fee to permanently remove a credit freeze (unless the consumer can provide a valid copy of an identity theft report filed with a law enforcement agency), to wit:

- $10.00 to permanently remove a credit freeze for residents of Alabama, Alaska, Arkansas, California, Colorado, Florida, Illinois, Iowa, Kansas, Kentucky, Maine, Michigan, Mississippi, Nevada, New Hampshire, North Carolina, Oklahoma, Oregon, Rhode Island, Utah, Washington, Wisconsin and Wyoming.

- $10.60 (including tax) to permanently remove a credit freeze for residents of Connecticut, South Carolina and South Dakota.

- $10.70 (including tax) to permanently remove a credit freeze for residents of Puerto Rico.

- $10.83 (including tax) to permanently remove a credit freeze for residents of Texas.

- $5.00 to permanently remove a credit freeze for residents of Arizona, Maryland, Massachusetts, Minnesota, New Jersey, Ohio, Tennessee and Vermont.

- $5.20 (including tax) to permanently remove a credit freeze for residents of Hawaii.

- $5.25 (including tax) to permanently remove a credit freeze for residents of New Mexico.
- $5.30 (including tax) to permanently remove a credit freeze for residents of West Virginia.
- $5.41 (including tax) to permanently remove a credit freeze for residents of New York.
- $3.00 (including tax) to permanently remove a credit freeze for residents of Georgia.

64. Upon information and belief, Equifax also charges similar fees to permanently lift a credit freeze.

65. As BNY's June 7, 2008 letter points out, "using a credit or credit freeze may delay your ability to obtain credit." Indeed, one of the credit reporting agencies (TransUnion) explains that a credit freeze means that "all third parties whose use is not exempt by law will be unable to access your credit report without your consent," and, as a consequence, the credit freeze "may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report." In addition, companies that provide consumer data to the credit reporting agencies will not be able to update the name and address information of consumers whose credit reports are frozen.

66. The June 7, 2008 BNY letter plainly states that there are expenses associated with credit freezes and unfreezes that are outside of the scope of BNY's remedial scheme: "[b]ecause credit or credit freezes can be temporarily removed on more than one occasion, you may incur costs associated with having a credit or credit freeze on your credit file *that BNY Mellon will not cover*." (emphasis supplied).

67. BNY's offer to pay for the initial placement and one removal of a credit freeze is wholly inadequate.

ii. The Unique Concerns and Problems Relating to Social Security Numbers are not Adequately Accounted for in the BNY Remedial Scheme.

68. In his May 30, 2008 press release, Connecticut Attorney General Blumenthal indicated that while there had been no reports of actual identity theft at that time, "the risk [of identity theft] may last for months or years." This risk is particularly serious in this case where Social Security numbers were among the compromised data. Unlike a data breach involving the theft of a consumers' credit or debit card information, which can simply and readily be canceled, the theft of a consumer's Social Security number puts that consumer at risk of identity theft for the rest of his or her life – and possibly even beyond.

69. Indeed, a June 2007 report issued by the United States Government Accountability Office discussed the two different types of identity theft, and explained why identity theft involving Social Security numbers are particularly serious:

> There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use identifying data, which can include such things as SSNs and driver's license numbers, to open new financial accounts and incur charges and credit in an individual's name, without that person's knowledge. *This second form of identity theft is potentially the most damaging because, among other things, it can take some time before a victim becomes aware of the problem, and it can cause substantial harm to the victim's credit rating.*[4]

70. This report also recognizes that Sensitive Personal Information – particularly Social Security numbers – can be used for improper purposes for several years.

> [L]aw enforcement officials told us that in some cases, stolen data

[4] http://www.gao.gov/new.items/d07737.pdf (emphasis supplied).

> may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.[5]

71. The Social Security Administration also cautions consumers about the perils of identity theft, and explains how a Social Security number can be misused without one's knowledge:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and do not pay the bills. You may not find out that someone is using your number until you are turned down for credit or you begin to get calls from unknown creditors demanding payment for items you never bought.[6]

72. Social Security numbers cannot be easily changed, and may even create a host of additional problems if a new number is assigned. In order to obtain a new Social Security number due to its misuse, one must contact the Social Security Administration and prove their age, U.S. citizenship or lawful immigration status, and "provide evidence that you still are being disadvantaged by the misuse." According to the Social Security Administration, a new Social Security number can create new problems because prior positive credit information is not associated with the new number, which may make it more difficult to obtain credit in the future due to the absence of a credit history. Further, employers, government agencies, private businesses and credit reporting agencies will likely have the person's old Social Security number. Two years worth of credit monitoring is not sufficient to adequately protect consumers' "lost" Social Security numbers.

---

[5] *Id.*

[6] http://www.socialsecurity.gov/pubs/10064.pdf

iii. Other Shortcomings of BNY's Remedial Scheme.

73. In addition to offering consumers an unreasonably abridged period of free credit monitoring and paying for the costs associated with a single credit freeze and unfreeze, BNY is not offering *any* identity theft insurance-type compensation to consumers in states (such as New York) where such insurance coverage is prohibited by applicable laws. The extent to which BNY will indemnify or protect consumers who live in such states – if at all – from identity theft as a result of its negligence, is unclear. Further, there is no alternative dispute resolution or other program offered by BNY whereby consumers who may have suffered actual identity fraud and/or out-of-pocket expenses to repair their credit as a result of BNY's wrongful actions and/or inaction may submit claims to BNY for reimbursement.

E. Sensitive Personal Information and its Misuse.

74. The effects of an unauthorized disclosure of confidential personal and financial information, such as that involved in the BNY data breaches, can be, and often are, serious and far-reaching. As noted by the President's Identity Theft Task Force, headed by the United States Department of Justice and the Federal Trade Commission, "any loss or theft of personal information is troubling and potentially devastating for the persons involved." *See* Combating Identity Theft: A Strategic Plan (April 2007) at 13.

75. The Sixth Circuit Court of Appeals similarly found in *U. S. v. Williams*, 355 F. 3d 893, 898 (6th Cir. 2003), that "[c]riminals use this information to establish credit in their name, run up debts on another person's account, or take over existing financial accounts." Moreover, possession of personal confidential information may also allow criminals to "breed" identities, that is, to obtain other forms of identification that may further enhance their ability to misuse another's identity.

76. Data breaches significantly raise the possibility that a person's identity will be misused by criminals. As reported by the United States Secret Service in March 2006, "[c]yber-crime has evolved significantly over the last two years, from dumpster diving and credit card skimming to full-fledged online bazaars full of stolen personal and financial information." Press Release, U.S. Secret Service, United States Secret Service's Operation Rolling Stone Nets Multiple Arrests (March 28, 2006), http://www.secretservice.gov.press/pub0906.pdf.

77. These online "bazaars" allow the easy and quick dissemination of stolen personal and financial information by and between criminals. "Large scale data breaches would be of no more concern than small scale identity thefts if criminals were unable to quickly and widely distribute the stolen information for fraudulent use[.] Such wide-scale global distribution of stolen information has been made possible for criminals with the advent of criminal websites … dedicated to the sale of stolen personal and financial information. These websites allow criminals to quickly sell the fruits of their ill-gotten gains to thousands of eager fraudsters worldwide, thereby creating a black market for stolen personal information." Peretti, Kimberly Kiefer, United States Dept. of Justice, Data Breaches: What the Underground World of "Carding" Reveals, forthcoming in Vol. 25, Santa Clara Computer and High Technology Journal, at 2.

78. The potential harms from an identity theft can be serious and long-term. One study found that the average victim of an unauthorized use of wrongfully disclosed personal and confidential information spends approximately 600 hours and $1,400 repairing his or her credit once violated. *See* Identity Theft Resource Center, Facts and Statistics (Sept. 2003), available at www.idtheftcenter.org/facts.html. The Justice Department reported in 2006 that "[t]he average amount of money involved in any type of identity theft in which there was a loss was $1,290."

See Baum, K., "Identity Theft, 2004," Bureau of Justice Statistics Bulletin (U. S. Dept. of Justice April 9, 2006) at 6.

79. Victims of identity theft also often suffer harms beyond simply direct financial harm, including denial of credit or utility services, increased difficulty in securing employment or housing, and higher insurance and credit rates. In some cases, an identity theft victim may even have a criminal record develop in his or her name. *See* Identity Theft: The Aftermath 2004 at 15, available at www.idtheftcenter.org ("Aftermath"). Other "costs include lost wages or vacation time, diminished work performance, increased medical problems [and] impact on family and friends." *Id*. at 13.

80. Although many people experience losses or other issues within a few months after a data breach, in many instances the problems will persist for a much longer period. Unlike the theft of tangible property, confidential personal information cannot be "retrieved" after it has fallen into another's hands. Thus, even after a victim has recovered from an incident of identity theft, he or she remains vulnerable. As one commentator put it, "with identity theft, the crime can continue, for personal information works like an 'access card' that cannot be readily deactivated." Daniel J. Solove, Identity Theft, Privacy, and the Architecture of Vulnerability, 54 Hastings L. J. 1227, 1246-47 (April 2003).

81. Further, it is often the case that a victim will not discover that his or her personal confidential information has been stolen and misused until long after an identity theft has taken place, and then only when they are denied credit or discover that their bank accounts have been emptied.

82. Among the most effective ways to prevent or limit the possible harm from a security breach, such as in this case, is to put into place for several years a program of identity

fraud prevention, detection and remediation. Such a program should include—at a minimum—daily monitoring of all three major credit reporting agencies, monitoring of internet chat rooms and directories, and sifting through online public records for signs of Social Security fraud, stolen credit card account trafficking, and other types of identification theft. Such a program, which is offered by several credit monitoring services, will greatly reduce the chance of actual identity theft from occurring, and enhance the chance of early detection in order to combat the risk of financial and other personal harm.

83. Equally important is the fact that Plaintiffs and the Class members have been robbed of the value of their Confidential Information. According to www.hrexpertonline.com, "[o]ver the past few years, the general public has begun to understand the intrinsic value of [confidential information]. The increase in fraud is a less desirable consequence of the tremendous advances in collecting and processing data to provide enhanced value."

84. Similarly, according to www.Biosmagazine.co.uk, "[c]ustomer and personnel data have been universally regarded as basic research tools with little or no intrinsic value of their own. The growth of a substantial black market for personal information changed all this. Identity theft is the fastest growing crime worldwide, and . . . the value of personal information ranges **from £2 to £50 a record, depending on the specific content. Like it or not, one of the primary tools of business - personal data, is now valuable, and is being targeted by modern cyber-criminals."** (emphasis supplied).

85. Here, BNY's failure to adequately protect the Sensitive Personal Information and timely and completely notify Plaintiffs and the Class members of the data breaches, including the nature and extent of the information lost, at the very least, (i) exposed Plaintiffs and the Class members to substantially greater risk of identity theft, and (ii) deprived them of information that

would have allowed them to protect themselves from at least some of the consequences of BNY's wrongful actions and/or inaction. More important, BNY's wrongful actions and/or inaction robbed Plaintiffs and the Class members of the value of their Sensitive Personal Information.

F. Federal Legislation and Regulations.

86. The Gramm-Leach-Bliley Act ("GLB") requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of personal information entrusted to them, including names, addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers. The GLB sets forth the minimum privacy protections mandated by financial services companies.

87. BNY is a "financial institution" within the definition of the GLB and implementing regulations.

88. Pursuant to Section 505 of the GLB, four of the eight federal agencies charged with its implementation promulgated regulations implementing the privacy and security provisions of the GLB: (i) 12 C.F.R. Part 30, App. B contains regulations of the Office of the Comptroller of the Currency, Treasury ("OCC"); (ii) 12 C.F.R. Part 208, App. D-2 and Part 225, App. 5 contain regulations of the Board of Governors of the Federal Reserve System ("Board"); (iii) 12 C.F.R. Part 364, App. B contains regulations of the Federal Deposit Insurance Corporation ("FDIC"); and (iv) 12 C.F.R. Part 570, App. B contains regulations of the Office of Thrift Supervision, Treasury ("OTS").

89. Following an extensive notice and comment period, the four agencies (OCC, Board, FDIC and OTS) issued Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines") setting forth minimum mandatory measures, including

response programs and customer notification procedures, that a financial institution *must* develop and implement in the event of an unauthorized access to or use of customer information.

90. The Security Guidelines require financial institutions to, *inter alia*, assess and address the following risks:

- reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;
- the likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and
- the insufficiency of policies, procedures, customer information systems and other arrangements in place to control risks.

91. The Security Guidelines direct every financial institution to "enter into a contractual commitment with its Service Providers [such as Archival Systems] to implement appropriate measures designed to protect against unauthorized access to or use of customer information."

92. The Security Guidelines give financial institutions "an affirmative duty" to protect their customers' information against unauthorized access or use. Notification of customers of a security incident involving unauthorized access is a key part of that duty.

93. At a minimum, the notification must be timely, given in a clear and conspicuous manner, describe what the institution has done to protect the customers' information from further unauthorized access and include a working telephone number staffed with trained personnel to respond to customer inquiries and requests for assistance.

94. The four agencies, OCC, Board, FDIC and OTS, specifically rejected the request made in the notice and comment period that compliance with the Security Guidelines create a "safe harbor" defense from class action lawsuits, citing to Section 507 of the GLB (stating that the Act does not exempt state laws that offer greater consumer protection than the Act).

95. In addition to the Security Guidelines, the Federal Trade Commission ("FTC"), another agency charged with implementing the privacy policies of the GLB, issued its "Safeguards Rules," which apply to financial institutions and other institutions handling confidential customer information. 16 C.F.R. Part 314, 67 Fed. Reg. 36493 (May 23, 2002).

96. The Safeguards Rules require financial institutions, including BNY, to develop a written information security plan that describes its program to protect customer information. The security plan must, at a minimum:

a) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

b) require service providers by contract to implement and maintain such safeguards; and

c) evaluate and adjust the information security program in light of the results of the testing and monitoring required by the regulations and material changes to the business operations or any other known circumstances.

CLASS ACTION ALLEGATIONS

97. Plaintiffs bring this action on behalf of themselves and as a class action, pursuant to FED. R. CIV. P. 23(a), (b)(2) and (b)(3), on behalf of all consumers whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April

2008 BNY data breaches. The Class specifically excludes BNY and its officers, directors, agents, and/or employees and the Court and Court personnel.

98. Plaintiffs seek to represent the following Nationwide Class:

> **Nationwide Class:** All persons in the United States whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.

99. In the alternative, and pursuant to Fed. R. Civ. P. 23(c)(5), Plaintiffs seek to represent the following state sub-classes:

> **California Sub-Class:** All persons in California whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.
>
> **Illinois Sub-Class:** All persons in Illinois whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.
>
> **Michigan Sub-Class:** All persons in Michigan whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.
>
> **New Jersey Sub-Class:** All persons in New Jersey whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.
>
> **New York Sub-Class:** All persons in New York whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.
>
> **Pennsylvania Sub-Class:** All persons in Pennsylvania whose Sensitive Personal Information was wrongfully accessed and/or compromised in the February 2008 and/or April 2008 BNY data breaches.

100. The Nationwide Class is comprised of millions of consumers, the joinder of whom in one action is impracticable if not impossible. The California, Illinois, Michigan, New Jersey, New York, and Pennsylvania Sub-Classes are likewise sufficiently large to make joinder

impracticable. Disposition of the claims in a class action will provide substantial benefits to all of the Parties and the Court.

101. The rights of each Class member were violated in precisely the same manner by BNY's uniform wrongful conduct.

102. Questions of law and fact common to the Classes predominate over questions that may affect individual Class members including, *inter alia*:

a. whether BNY was negligent or negligent *per se* in collecting and storing the Sensitive Personal Information of Plaintiffs and the Class members;

b. whether BNY took reasonable measures to safeguard the Sensitive Personal Information of Plaintiffs and the Class members;

c. whether BNY owed a duty to Plaintiff and/or the Class members to protect their Sensitive Personal Information;

d. whether BNY breached its duty to exercise reasonable care in storing the Sensitive Personal Information of Plaintiffs and the Class members by, *inter alia*, failing to select a competent courier to transport the Sensitive Personal Information, failing to store the Sensitive Personal Information in an encrypted format and failing to adequately and properly supervise and monitor its couriers;

e. whether BNY breached its duty to Plaintiff and the Class members by failing to properly safeguard their Sensitive Personal Information;

f. whether BNY's actions and/or inaction violated California, Illinois, Michigan, New Jersey, New York, and Pennsylvania law;

g. whether Plaintiffs and the Class members are entitled to compensation, monetary damages and/or additional services/corrective measures from BNY and, if so, the nature and amount of any such relief; and

h. whether statutory and/or treble damages are proper in this matter.

103. Plaintiffs will fairly and adequately represent and protect the interests of the Classes in that they have no interests antagonistic to, or in irreconcilable conflict with, the interests of the other Class members.

104. Plaintiffs have retained counsel competent and experienced in the prosecution of class action and data breach litigation.

105. BNY has acted or refused to act on grounds generally applicable to Plaintiffs, the Nationwide Class and the State Sub-Classes, thereby making appropriate equitable relief with respect to Plaintiffs and the Classes as a whole.

106. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiffs' and Class members' claims. Plaintiffs and the members of the Nationwide Class and/or State Sub-Classes have suffered (and will continue to suffer) irreparable harm as a result of BNY's deceptive, negligent and unlawful conduct. The damages suffered by individual Class member is relatively small, and thus, few, if any, individual Class members can afford to seek legal redress on an individual basis for the wrongful conduct complained of herein. Absent a class action, Plaintiffs and the Class members will continue to suffer losses and not be adequately protected and compensated therefore.

CLAIMS FOR RELIEF/CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class or, Alternatively, On Behalf of the Individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes)

107. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

108. Plaintiffs assert this cause of action on behalf of themselves and the Nationwide Class or, in the alternative, on behalf of the individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes.

109. By having possession, custody and control over Plaintiffs' and the Class members' Sensitive Personal Information, BNY had a duty to exercise reasonable care to safeguard and protect such information from being compromised and/or stolen. BNY's duty arises from the common law, as well as from those duties expressly imposed upon BNY from other sources, such as contracts between Plaintiffs, the Class members and/or third parties, agreements between BNY and third parties and industry standards.

110. BNY also had a duty to timely and accurately disclose to Plaintiff and the Class members that their Sensitive Personal Information within BNY's possession, custody and control had been, or was reasonably believed to be, compromised, as well as the nature and extent of the information compromised.

111. BNY also had a duty to put into place policies and procedures to detect and prevent the unlawful and unauthorized dissemination of Plaintiffs' and the Class members'

Sensitive Personal Information to third parties. The February 2008 and April 2008 data breaches were reasonably foreseeable by BNY.

112. BNY, by its wrongful actions and/or inaction, breached its duties to Plaintiffs and the Class members by, *inter alia*, failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and the Class members' Sensitive Personal Information within its possession, custody and control.

113. BNY, by its wrongful actions and/or inaction, also breached its duties to Plaintiffs and the Class members by, *inter alia*, failing to put into place adequate procedures to detect and prevent the unlawful and unauthorized dissemination of Plaintiffs' and the Class members' Sensitive Personal Information to third parties. BNY also breached its duties to Plaintiffs and the Class members by storing (or causing to be stored) the Sensitive Personal Information of Plaintiffs and the Class members in an unencrypted, readily accessible format.

114. BNY, by its wrongful actions and/or inaction, also breached its duties to Plaintiffs and the Class members by, *inter alia*, failing to timely and accurately disclose to Plaintiff and the Class members that their Sensitive Personal Information within BNY's possession, custody and control had been, or was reasonably believed to be, compromised, as well as the nature and extent of the information compromised.

115. But for BNY's negligent and wrongful breach of the duties it owed to Plaintiffs and the Class members, their Sensitive Personal Information would not have been compromised. Further, but for BNY's belated and incomplete revelations about the data breaches, Plaintiffs and the Class members could have better protected themselves from the risk of identity theft and fraud.

116. Plaintiffs' and the Class members' Sensitive Personal Information was compromised, viewed and/or stolen as the direct and/or proximate result of BNY failing to exercise reasonable care in safeguarding such information by adopting, implementing and/or maintaining appropriate security measures to protect and safeguard the Sensitive Personal Information within its possession, custody or control.

117. Plaintiffs and the Class members have incurred and/or can be expected to incur actual damages including, but not limited to: expenses to prevent and/or repair identity theft, expenses associated with freezing and unfreezing their credit reports, expenses for identity theft coverage (or similar relief) for residents of New York and the residents of other similarly affected states, credit monitoring for an extended period of time, anxiety, emotional distress, loss of privacy, loss of peace of mind, the increased exposure to identity theft, and other economic and non-economic harm.

COUNT II

BREACH OF IMPLIED CONTRACT

(On Behalf of the Nationwide Class or, Alternatively, On Behalf of the Individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes)

118. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

119. Plaintiffs assert this cause of action on behalf of themselves and the Nationwide Class or, in the alternative, on behalf of the individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes.

120. Plaintiffs and the Class members were required to provide BNY with their Sensitive Personal Information in exchange for BNY providing its services to them. Implicit in

this transaction was a covenant requiring BNY to, *inter alia*, take reasonable efforts to safeguard the Sensitive Personal Information, and take appropriate measures to promptly notify consumers in the event the Sensitive Personal Information was compromised. Indeed, BNY recognizes these obligations since it issued policies and notices that inform consumers that BNY takes the protection of their Personal Sensitive Information "very seriously."

121. The implied contract between the Parties also required BNY to not disclose Plaintiffs' and the Class members' Sensitive Personal Information and safeguard and protect the Sensitive Personal Information from being compromised and/or stolen.

122. BNY, however, did not safeguard and protect Plaintiffs' and the Class members' Sensitive Personal Information from being compromised and/or stolen. To the contrary, BNY allowed this information to be disclosed to multiple unauthorized third parties.

123. BNY breached its implied contract with Plaintiffs and the Class members by, *inter alia*, unlawfully disseminating and/or allowing to be disseminated their Sensitive Personal Information, failing to timely and thoroughly inform Plaintiffs and the Class members of the data breaches, including the nature and extent of the information lost, and failing to safeguard and protect Plaintiffs' and the Class members' private, nonpublic and Sensitive Personal Information from being compromised and/or stolen.

124. Plaintiffs and the Class members have incurred and/or can be expected to incur actual damages including, but not limited to: anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

COUNT III

BREACH OF FIDUCIARY DUTY

(On Behalf of the Nationwide Class or, Alternatively, On Behalf of the Individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes)

125. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

126. Plaintiffs assert this cause of action on behalf of themselves and the Nationwide Class or, in the alternative, on behalf of the individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes.

127. By virtue of its possession, custody and/or control of Plaintiffs' and the Class members' Sensitive Personal Information, BNY was entrusted with, among other things, the duty and obligation to monitor and safeguard their Sensitive Personal Information and timely and completely notify them of any data breaches wherein their Sensitive Personal Information was stolen and/or compromised. BNY accepted this relationship of trust and confidence for which it was compensated handsomely.

128. By virtue of its possession, custody and/or control of Plaintiffs' and the Class members' Sensitive Personal Information, and its duty to properly monitor and safeguard such Sensitive Personal Information, BNY was (and continues to be) in confidential, special and/or fiduciary relationships with Plaintiffs and the Class members. As a fiduciary, BNY owed (and continues to owe) to Plaintiffs and the Class members (i) the commitment to deal fairly and honestly, (ii) the duties of good faith and undivided loyalty, and (iii) integrity of the strictest kind. BNY was (and continues to be) obligated to exercise the highest degree of care in carrying out its responsibilities to Plaintiffs and the Class members under such confidential, special and/or fiduciary relationships.

129. BNY breached its fiduciary duties to Plaintiffs and the Class members by, *inter alia,* (i) improperly and negligently storing, monitoring and/or safeguarding Plaintiffs' and the Class members' Sensitive Personal Information, (ii) failing to timely and completely notify Plaintiffs and the Class members of the data breaches and the nature and extent of the information lost, (iii) failing to take adequate steps in advance to prevent the data breaches that it eventually took after the data breaches occurred, and (iv) failing to take adequate steps to reduce or eliminate the risk and consequences of the misuse of the compromised Sensitive Personal Information.

130. BNY breached its fiduciary duties to Plaintiffs and the Class members by its wrongful actions and/or inaction described above. BNY willfully and wantonly breached its fiduciary duties to Plaintiffs and the Class members or, at the very least, committed these breaches with conscious indifference and reckless disregard of their rights and interests. BNY's wrongful actions and/or inaction, in turn, caused Plaintiffs and the Class members to suffer damages.

COUNT IV

NEGLIGENCE *PER SE*

(On Behalf of the Nationwide Class or, Alternatively, On Behalf of the Individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes)

131. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

132. Plaintiffs assert this cause of action on behalf of themselves and the Nationwide Class or, in the alternative, on behalf of the individual California, Illinois, Michigan, New Jersey, New York and Pennsylvania Sub-Classes.

133. BNY violated numerous provisions of the regulations implementing the GLB, including:

a. failure to maintain policies, procedures, customer information systems, and other arrangements to control costs;

b. failure to implement appropriate measures with its service providers to protect against unauthorized access;

c. failure to notify consumers in a timely manner;

d. failure to adequately assess or address the risk of transporting unencrypted tapes taking into account the sensitivity of consumer information;

e. failure to describe what it did to protect the consumers' information from further unauthorized access; and

f. failure to evaluate and adjust its program as the results of security breaches.

134. The regulations promulgated by the federal agencies charged with implementing the GLB (*i.e.*, the "Security Guidelines" issued by OCC, the Board, FDIC and OTS and the Safeguards Rules issued by the FTC) establish a minimal duty of care owed by BNY to Plaintiffs and the Class members.

135. BNY failed to meet its minimal duty under the GLB regulations.

136. BNY also failed to satisfy the minimal duty set forth in the Pennsylvania Breach of Personal Information Notification Act ("BPINA"). The BPINA requires entities that maintain or store computerized data, including Sensitive Personal Information, to provide notice "without unreasonable delay" following the discovery of a data breach to any resident of Pennsylvania who's unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person. 73 P.S. § 2303(a). BNY failed to notify Plaintiff Young and the Pennsylvania Sub-Class members about the data breaches without unreasonable delay pursuant to this statute.

137. BNY's violations of the BPINA caused injury to Plaintiffs and the Class members.

138. Further, and pursuant to New York State General Business Law § 899-aa, "any person which conducts business in N.Y. state . . . must following a security breach that compromises "private information" (defined as social security number, . . . or account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account) to disclose the breach to the affected person "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." § 899-aa.2.

139. BNY's wrongful conduct also violated N.Y. GEN. BUS. LAW § 899-aa, *et seq*, because BNY failed to timely and completely notify Plaintiff Wicks and the New York Sub-Class members of the data breaches and that their Sensitive Personal Information was acquired – or was reasonably believed to have been acquired – by an unauthorized person and compromised.

140. The injuries suffered by Plaintiffs and the New York Sub-Class members were of the type intended to be prevented by these and other statutes.

141. Plaintiffs and the Class members are members of the classes of persons intended to be protected by these and other similar state statutes.

142. BNY's negligence *per se* is a direct and/or proximate cause of the resulting injuries to Plaintiffs and the Class members.

COUNT V

CALIFORNIA UNFAIR COMPETITION LAW
(BUS. & PROF. CODE §17200, *ET SEQ*.)

(On Behalf of the California Sub-Class)

143. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

144. Plaintiff Bernstein asserts this cause of action on behalf of herself and the California Sub-Class.

145. BNY engaged in unfair, unlawful and fraudulent business practices in that (i) BNY's unlawful conduct violated federal, state, regulatory and/or industry standards, as described herein, (ii) the justification for BNY's conduct is outweighed by the gravity of the consequences to Plaintiff and the California Sub-Class, and (iii) BNY's conduct is immoral, unethical, oppressive, unscrupulous or substantially injurious to Plaintiff and the California Sub-Class. Such conduct violates California Business & Professions Code § 17200, *et seq.* By engaging in the above-described acts and practices, BNY committed one or more acts of unfair competition within the meaning of California Business & Professions Code §17200, *et seq*.

146. BNY's acts and practices deceived and/or are likely to deceive the consuming public and the California Sub-Class.

147. The injury to consumers by BNY's wrongful conduct greatly outweighs any alleged countervailing benefit to consumers or competition under all of the circumstances. Moreover, the injury is not one that Plaintiff and the California Sub-Class could have reasonably avoided.

148. Plaintiff Bernstein, on behalf of herself and the California Sub-Class, therefore, seeks an order from this Court awarding restitution, disgorgement, injunctive relief and all other

relief allowed under California Business & Professions Code Section 17200 *et seq*., plus interest, attorneys' fees, expenses and costs.

COUNT VI

VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT (MCL 445.901, *ET. SEQ.*)

(On Behalf of the Michigan Sub-Class)

149. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

150. Plaintiff Hammond asserts this cause of action on behalf of himself and the Michigan Sub-Class.

151. Plaintiffs entrusted their Sensitive Personal Information to BNY primarily for their personal, family and household purposes.

152. BNY's wrongful conduct alleged herein violates the Michigan Consumer Protection Act, MCL 445.901, *et. seq.*, including, but not limited to, the following sections:

a) § 445.903(s), by failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer.

b) § 445.903(bb), by making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is.

c) § 445.903(cc), by failing to reveal facts which are material to the transaction in light of representations of fact made in a positive manner.

153. Plaintiff Hammond, nor any other Michigan Sub-Class member, would have entrusted or consented to providing their Sensitive Personal Information to BNY had they known, *inter alia*, that BNY would not take adequate measures to protect this highly sensitive and confidential information and, in the event of a data breach, BNY would not give timely notice or take appropriate and meaningful measures to adequately compensate and protect consumers.

154. As a result of BNY's violation of the Michigan Consumer Protection Act, Plaintiff Hammond and the Michigan Sub-Class have incurred damages and, as a result, demand actual, statutory, and treble damages.

COUNT VII

VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT ("CFA") (N.J.S.A. § 56:8-1, *ET SEQ*.)

(On Behalf of the Nationwide Class or, Alternatively, On Behalf of the New Jersey Sub-Class)

155. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

156. Plaintiffs Giordano and Wood assert this cause of action on behalf of themselves and the Nationwide Class and, in the alternative, the New Jersey Sub-Class.

157. Plaintiffs Giordano, Wood and the other Nationwide and/or New Jersey Sub-Class members are "persons" within the meaning of the CFA.

158. Plaintiffs Giordano, Wood and the other Nationwide and/or New Jersey Sub-Class members also are "consumers" within the meaning of the CFA.

159. At all relevant times, BNY conducted trade and commerce in New Jersey and

elsewhere within the meaning of the CFA. Upon information and belief, the unencrypted tapes lost in the February 2008 data breach were lost while in transit in New Jersey. The CFA, by its terms, is a cumulative remedy, such that its remedies can be awarded in addition to those provided under separate statutory schemes.

160. BNY engaged in deceptive practices by, *inter alia*, failing to disclose the data breaches, delaying any disclosure of the data breaches and/or withholding material facts from its communications and disclosures to Plaintiffs Giordano, Wood and the other Nationwide and/or New Jersey Sub-Class members regarding the nature and extent of the data breaches.

161. BNY's foregoing actions, inaction, misrepresentations, omissions and unconscionable commercial practices caused Plaintiffs Giordano, Wood and the other Nationwide and/or New Jersey Sub-Class members to suffer an ascertainable loss and other damages, which they now seek to recover.

COUNT VIII

VIOLATION OF SECTION 349 OF THE NEW YORK GENERAL BUSINESS LAW

(On Behalf of the New York Sub-Class)

162. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as if fully set forth herein.

163. Plaintiff Wicks and Plaintiff Kanney assert this cause of action on behalf of themselves and the New York Sub-Class.

164. Plaintiff Wicks and Plaintiff Kanney are consumers who reside in New York.

165. BNY engaged in unfair and deceptive practices, as described herein, in violation of Section 349 of the New York General Business Law.

166. BNY's unfair and deceptive practices directly and/or proximately caused damages to Wicks, Kanney, and the other New York Sub-Class.

COUNT IX

VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE PRACTICES ACT, ("CFDPA") (ILL. COMP. STAT. ANN. 505/1 AND 510/1, *ET SEQ*.)

(On Behalf Of the Illinois Sub-Class)

167. Plaintiffs repeat and reallege the allegations of the preceding paragraphs as If fully set forth herein.

168. Witek asserts this cause of action on behalf of himself and the Illinois Sub-Class.

169. At all relevant times, Witek and the Illinois Sub-Class were consumers within the meaning of CFDPA.

170. At all relevant times hereto, BNY engaged in trade and/or commerce within the meaning of CFDPA.

171. Under the circumstances, BNY's representations, delayed disclosure, and omissions regarding the data breaches were misleading and deceptive. BNY intentionally made these misleading and deceptive representations and/or omissions (while knowing they were deceptive and misleading) for the sole purpose of deceiving Witek and the Illinois Sub-Class. BNY intended that Witek and the Illinois Sub-Class rely on BNY's deceptive and misleading practice.

172. BNY's conduct was unfair and deceptive and constituted an improper concealment, suppression and/or omission of material facts, in violation of the CFDPA's prohibition against unfair business practices.

173. BNY violated the CFDPA's prohibition against misrepresenting and/or omitting

material information during commercial transactions, as well as the CFDPA's prohibition against unfair business practices. This misconduct took place in the course of trade or commerce in Illinois.

174. As a direct and proximate result of BNY's violations of the CFDPA, Witek and the Illinois Sub-Class suffered damages.

REQUEST FOR RELIEF

175. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if fully set forth herein.

176. **ACTUAL DAMAGES.** As a direct and/or proximate result of BNY's wrongful actions and/or inaction, Plaintiffs and the Class members have sustained (and will continue to sustain) damages in the form of, *inter alia*, the (i) theft of the value of their Sensitive Personal Information that was improperly stolen, misplaced and/or compromised, (ii) unauthorized disclosure and/or compromise of their Sensitive Personal Information, (iii) monetary losses for money stolen from their accounts and/or fraudulent charges made on their accounts, (iv) value of all time expended and/or out-of-pocket expenses incurred to proactively safeguard and/or repair their credit and/or restore their identities including, *inter alia*, closing and re-opening checking accounts and debit/credit card accounts, credit freezing and unfreezing, and similar changes to other accounts, and (v) the burden and expense of comprehensive credit monitoring for more than two (2) years into the future. All of Plaintiffs' and Class members' damages were reasonably foreseeable by BNY.

177. **EQUITABLE RELIEF.** Plaintiffs and the Class members are entitled to equitable and injunctive relief; to wit, creation of a fund for comprehensive credit monitoring for more than two (2) years into the future, as well as identification theft prevention and remediation

purposes including, *inter alia*, the appointment of an administrator and an advisory panel of persons qualified and knowledgeable in the field of identity theft detection, prevention and remediation to oversee the fund so as to prevent any additional harm and remedy actual harm that has or will occur.

178. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COURT COSTS.** Plaintiffs and the Class members also are entitled to recover their reasonable and necessary attorneys' fees, litigation expenses and court costs through the trial and any appeals of this case.

****

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated members of the putative Classes, respectfully request that this Court (i) certify this action as a Nationwide Class action and/or certify the individual State Sub-Classes, (ii) appoint them as the named representatives of the Classes, (iii) appoint their attorneys as Class Counsel, and (iv) upon final trial or hearing:

(i) enter judgment in favor of Plaintiffs and the certified Class(es) against BNY under the legal theories alleged herein in the types and amounts to be determined by the trier of fact;

(ii) award equitable relief to Plaintiffs and the Class members, as described above;

(iii) award to Plaintiffs and the Class members their reasonable and necessary attorneys' fees, litigation expenses and costs of suit;

(iv) award to Plaintiffs and the Class members pre-judgment and post-judgment interest at the maximum rates allowed by law; and

(v) award to Plaintiffs and the Class members such other and further relief to which they are justly entitled.

JURY DEMAND

Plaintiffs, on behalf of themselves and the putative Classes, demand a trial by jury on all issues so triable.

Dated: April 22, 2009

Respectfully submitted,

By: _____

Joseph G. Sauder (admitted *pro hac vice)*
Matthew D. Schelkopf (PA ID 89143)
Benjamin F. Johns (admitted *pro hac vice*)
CHIMICLES & TIKELLIS, LLP
One Haverford Centre
361 West Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
E-mail: JosephSauder@chimicles.com
matthewschelkopf@chimicles.com
BFJ@chimicles.com

Christopher G. Hayes (PA ID No. 57253)
LAW OFFICE OF
CHRISTOPHER G. HAYES
225 South Church Street
West Chester, PA 19382
Telephone: (610)-431-9505
Facsimile: (610)-431-1269
E-mail: chris@chayeslaw.com

Judith Scolnick
SCOTT + SCOTT, LLP
29 West 57th Street
New York, NY 10019
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
E-Mail: jscolnick@scott-scott.com

Attorneys for Plaintiffs and the Proposed Classes

EXHIBIT A

State of Connecticut

RICHARD BLUMENTHAL
ATTORNEY GENERAL

Hartford
May 21, 2008

VIA ELECTRONIC MAIL AND FIRST CLASS U.S. MAIL

Stephen Dalmatch
General Counsel
Bank of New York Mellon Shareowner Services
480 Washington Avenue
Jersey City, NJ 07310

RE: The Bank of New York Mellon Security Breach -- Missing Back-up Tapes

Dear Mr. Dalmatch:

I am alarmed and deeply concerned by a recent and serious data breach at The Bank of New York Mellon ("BNY") involving the loss of computer back-up tapes containing sensitive information of some 4.5 million consumers, including People's United Bank account holders and shareowners Several hundred thousand Connecticut citizens may be affected, and possibly more, by this loss of highly significant personal information.

BNY representatives informed my office that the information on the tapes contained, at a minimum, Social Security numbers, names and addresses, and possibly bank account numbers and balances. I am especially concerned about the possibility that credit card fraud and identity loss may result from the breach of this sensitive and personally identifying information

According to the information you provided, a metal box with six to ten unencrypted back-up bank tapes containing confidential personal information was "lost" in February, 2008 from a truck owned by Archival Systems, Inc., a company that transports and "securely" stores these types of tapes in its storage facility. The lock on the truck was broken -- possibly before the beginning of the workday -- and the truck was left unattended several times Ten boxes from BNY were placed on the truck. Only nine reached the storage facility.

This security breach seems highly dangerous, indeed possibly devastating in light of the identity theft threat You have also informed this office that BNY began notifying the affected customers six weeks ago and is offering one year of credit monitoring through Equifax. Given this extraordinarily serious security breach, this offer of protection is grossly inadequate Connecticut agencies that have experienced data security breaches less serious in magnitude or

potential damage have offered consumers two years of credit monitoring, $25,000 identity theft insurance and free credit freezes BNY should do no less

Given the possible devastating impact on consumers in Connecticut, my office requests more detailed information -- in full and in writing -- on how this breach occurred, what steps have been taken to protect these individuals, and what new procedures have been adopted to prevent future data breaches.

For the purposes of this letter and the questions below, "You" and "Your" refer to BNY Please provide responses to the following by May 30, 2008:

1 Prior to the loss of this data, what measures did You take to safeguard sensitive information of the sort contained on the lost back-up tapes;

2 Please indicate how and when You first learned of the loss of the back-up tapes;

3 Please describe in detail the circumstances under which the back-up tapes were lost;

4. Please identify the total number of Connecticut consumers that may possibly be affected by the loss of the back-up tapes;

5 Please identify each issuer (client of Yours) which had its clients/shareholders/customers' information on one of the missing back-up tapes and, for each, identify the number of Connecticut residents that may possibly be affected by the loss of the back-up tapes;

6. Please describe in detail the categories of consumer information compromised by the loss including, but not limited to, name, address, Social Security Number, or other sensitive information;

7 Please describe all steps that You have taken to track down and retrieve the missing back-up tapes and the sensitive files and information contained thereon;

8 Please describe all steps You have taken or will take to contact and warn consumers that their sensitive and personally identifying information may have been compromised including, but not limited to, when and how You first notified consumers of this loss, and whether You will individually notify each consumer about the loss;

9 Please identify all steps You have taken or will take to protect those consumers whose personal information may have been or was actually compromised from

identity theft and credit card fraud, including, but not limited to, any credit monitoring or identity restoration services and insurance that has been or will be offered to these consumers;

10. Please provide an outline of the plan You have developed to prevent the reoccurrence of such a loss and a timeline for implementing that plan;

11 Please describe Your general corporate policies regarding securing back-up tapes such as the lost tapes that are the subject of this letter, and the personally identifying information contained thereon; and

12. Please identify each instance where a back-up tape was lost in the past and, for each incident, state whether such tape contained any sensitive, personally identifiable information

I am especially concerned by the delay in informing consumers, possibly heightening the risks of wrongdoing. Neither People's nor its customers were promptly notified. Even now, many may be in the dark.

The loss of these tapes -- so far unrecovered and unremedied -- is inexplicable and unacceptable. It must be addressed by protective measures to forestall identity theft immediately

I appreciate your cooperation in this matter and look forward to hearing from you. The information requested herein should be sent to Assistant Attorneys General Matthew Fitzsimmons and Phillip Rosario at 110 Sherman Street, Hartford, Connecticut 06105 Should you have any questions, you may contact Assistant Attorneys General Fitzsimmons or Rosario at (860) 808-5400. Thank you

Very truly yours,

RICHARD BLUMENTHAL

RB/pas

EXHIBIT B

THE BANK OF NEW YORK MELLON

June 7, 2008

Dear MetLife Customer:

The Bank of New York Mellon processes payments on behalf of MetLife and other corporate customers. The Bank receives documents through the mail, among them checks from employers and accompanying remittance slips.

The Bank was recently advised that an unencrypted back-up tape containing images of these documents and other items that the Bank processed during the period February 25 to April 25, 2008, was lost while being transported by an outside carrier from the Bank's processing site in Philadelphia, PA to its data storage site in Pittsburgh, PA. The images may include personal information about you, such as name, address and social security number. Please bear in mind that these were images and not the original documents themselves.

Based on our investigation and information available to date, it appears that the tape was lost in transit. We have no reason to believe that the tape was stolen, or that unauthorized persons have accessed any information on the tape. **Also, please be assured that this incident did not affect the deposit and crediting of your annuity payments.**

Safeguarding confidential customer data is a top priority at The Bank of New York Mellon. We are implementing additional security procedures to help ensure that an event such as this does not occur again.

As an added precaution to help detect any possible misuse, we are offering you credit report monitoring services for two years, at no cost. We have engaged ConsumerInfo.com, Inc., an Experian® Company, to provide you with their Triple Alert℠ Credit Monitoring product. This includes daily monitoring of credit reports from three major consumer reporting companies (Equifax®, Experian® and TransUnion®), e-mail monitoring alerts of key changes to your credit reports and more.

Through Experian®, we are also offering, without charge, Identity Theft Insurance in the amount of $25,000 through Virginia Surety Company, Inc. with no deductible. (Note: Due to New York state law restrictions, Identity Theft Insurance coverage cannot be offered to residents of New York. Daily monitoring of credit reports, however, is available to New York residents.)

The free credit monitoring service and Identity Theft Insurance must be activated within 90 days of the date of this letter. To enroll, you should call us, toll-free at 1-877-279-1093. Our customer service representatives are available Monday through Friday, between the hours of 8 a.m. and 8 p.m. ET and Saturday, between the hours of 9 a.m. and 4 p.m. ET. When you call, you will be provided an activation code. This code is only for your use. With the activation code, you may then enroll with our customer service representative. You may also enroll online at **http://partner.experiandirect.com/triplealert**.

You may also wish to place a credit or security freeze on your consumer credit files. A credit or security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. **However, using a credit or security freeze may delay your ability to obtain credit.** You may request that a freeze be placed on your consumer report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address on the next page.

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.com
(800) 685-1111	(888) 397-3742	(888) 909-8872

The following information should be included when requesting a credit or security freeze (documentation for you and your spouse must be submitted when freezing a spouse's consumer report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request also should include a copy of a government issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The consumer reporting agency may charge a reasonable fee to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the consumer reporting company. If you place a credit or security freeze within 90 days of the date of this letter, the Bank of New York Mellon will cover the cost of the initial placement and one removal (whether a temporary or permanent removal) of a credit or security freeze even if you are not the victim of identity theft. Because credit or security freezes can be temporarily removed on more than one occasion, you may incur costs associated with having a credit or security freeze on your credit file that BNY Mellon will not cover. Additional details on the credit or security freeze process, and how you may have BNY Mellon cover the charges, will be provided when you call the toll-free number below.

In all events, we recommend that you remain vigilant and take measures to regularly review and monitor your financial accounts to determine if there are any unauthorized transactions. If you detect any unauthorized transactions, promptly notify your financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities and to the Federal Trade Commission. You can learn more about how to protect yourself from becoming a victim of identity theft at the FTC's website: **www.ftc.gov/bcp/edu/microsites/idtheft/index.html**

In addition, we recommend that you obtain a copy of your credit report from one or more of the national credit reporting companies. You may receive a free credit report once every 12 months through the Annual Credit Report Service by visiting **www.annualcreditreport.com** or calling, toll-free to 877-322-8228, or by calling one of the three national credit reporting companies, toll free: Experian® at 888-397-3742; Equifax® at 800-685-1111; and TransUnion® at 800-916-8800.

You may also wish to place a "fraud alert" on your consumer credit files by contacting any of the three nationwide consumer reporting companies. A fraud alert means that creditors should take additional steps to verify the identity of anyone who applies for credit in your name, and should also reduce the possibility of identity theft. There is no charge for placing a fraud alert on your consumer credit files. You may place a fraud alert by contacting any of the credit reporting companies using the information provided above.

If you would like additional information or further assistance regarding this matter, please call us, toll-free at 1-877-279-1093.

We sincerely regret any inconvenience or concern this matter may have caused you.

Sincerely,

The Bank of New York Mellon

EXHIBIT C

BNY MELLON SHAREOWNER SERVICES
Attn: SHAREOWNER SERVICES
PO BOX 1690
Manchester, CT 06045

BNY MELLON
SHAREOWNER SERVICES

1-866-926-9805

THOMAS CARROLL HAMMOND
2700 GLENROSE ST
AUBURN HILLS
MI 48326

May 27, 2008

Dear Sir or Madam:

BNY Mellon Shareowner Services provides stock transfer agency, employee plan administration and related services for issuers of securities such as publicly traded corporations. While we have no reason to believe your information has been or will be accessed or misused, we are writing to inform you of an incident involving your personal information that we maintain in connection with these services. On February 27, 2008, our archive services vendor notified us that they could not account for one of several boxes of data backup tapes that they were transporting to an off-site storage facility. The missing tapes contained certain personal information, such as your name, address, Social Security number and/or shareowner account information, that we maintain in providing these services.

Although we have no indication of any improper access to this data, as a precaution, to help you detect any possible misuse of your data, we are offering you free credit monitoring for a 12-month period. We have engaged ConsumerInfo.com, Inc., an Experian® Company, to provide you with their Triple Alert℠ Credit Monitoring product, which includes daily monitoring of your credit reports from three national credit reporting companies (Experian, Equifax® and TransUnion®), email monitoring alerts of key changes to your credit reports, and more.

For more information, please visit our website at **http://www.bnymellon.com/tapequery**. You have 90 days from the date of this notice to activate the credit monitoring by using the **activation code** [redacted] This code is unique for your use and should not be shared. To learn more about Triple Alert℠ and to enroll, go to **http://partner.consumerinfo.com/monitor** and follow the instructions. To enroll by phone, or if you have any questions, please call us **toll-free at 1-877-278-3458**. Our customer service representatives are available Monday through Friday, between 8 a.m. and 8 p.m. ET; and Saturday, between 9 a.m. and 4 p.m. ET.

We recommend that you regularly review statements from your accounts and obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by visiting http://www.annualcreditreport.com or by calling one of the three national credit reporting companies, toll-free: Experian at (888) 397-3742; TransUnion at (800) 916-8800; Equifax at (800) 685-1111. We recommend you remain vigilant and that you report any suspected identity theft to us and to proper law enforcement authorities, including the Federal Trade Commission. Please visit the FTC's web site, http://www.ftc.gov/bcp/edu/microsites/idtheft, to learn more about protecting yourself from identity theft, such as requesting a fraud alert.

Please be assured that we take the protection of your information very seriously and have taken additional measures to protect your account with us. We have implemented additional measures that will help prevent a similar occurrence. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

BNY Mellon Shareowner Services

CERTIFICATION

I, Benjamin F. Johns, certify that on this 22nd day of April 2009, I served the persons listed below with the foregoing **PLAINTIFFS' SECOND AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND** (and the exhibits thereto) via first class U.S. mail and via electronic mail to the foregoing parties:

Stephen L. Ratner, Esquire
Margaret Dale, Esquire
Doug Rennie, Esquire
PROSKAUER ROSE LLP
1585 Broadway
New York, NY 10036-8299

By: /s/ Benjamin F. Johns
Benjamin F. Johns